Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1. (currently amended) A computing device comprising:

a processing system;

an externally-accessible memory coupled to the processing system;

a secret identification number generated for the computing device and stored in a secure memory that is not externally-accessible;

a key generator for generating a random key associated with a selected electronic file to be stored in the externally-accessible memory;

a symmetrical encryption system to generate an encrypted key by symmetrically encrypting the random key using the secret identification number;

wherein the processing system associates a digital certificate with ~~the~~ an electronic file, where the digital certificate contains the encrypted key, such that the electronic file can be accessed only after the processing system restores the random key through decryption of the encrypted key with the secret identification number;

wherein the random key is used to sign the file certificate, the electronic file is optionally encrypted using the random key, the electronic file is accessed when the file certificate is verified using the random key and the encrypted electronic file is decrypted using the random key; and

the externally-accessible memory further comprising an asymmetric manufacture certificate to bind firmware to the processing system.

Claim 2. (currently amended) The computing device of claim 1 wherein digital certificate ~~comprises~~ contains a software signature that is symmetrically encrypted using the random key; wherein the software signature is a signature for the electronic file that is symmetrically encrypted using the random key.

Claim 3. (original) The computing device of claim 2 wherein the software signature comprises a hash of the electronic file, where the hash is symmetrically encrypted using the random key.

Claim 4. (currently amended) The computing device of claim 2 wherein the digital ~~signature~~ certificate further contains a signature for selected fields of the digital certificate, wherein the selected fields of the digital certificate are hashed ~~coded~~ and encrypted using the random key.

Claim 5. (original) The computing device of claim 1 wherein the electronic file is symmetrically encrypted using the random key.

Claim 6. (currently amended) The computing device of claim 1, wherein the encrypted ~~encoded~~ key is stored in the externally-accessible memory.

Claim 7. (currently amended) A method of providing security to files stored in an externally-accessible memory of a computing device comprising the steps of:

storing a secret identification number for the computing device in a secure memory that is not externally-accessible;

generating a random key;

generating an ~~encoded~~ encrypted key by symmetrically encrypting the random key using the secret identification number;

associating a digital certificate with the electronic file, where the digital certificate contains the encrypted key, such that the electronic file can be accessed only after restoring the random key through decryption of the encrypted key with the secret identification number;

using the random key to sign the file certificate, and optionally encrypting the electronic file using the random key, and wherein the electronic file is accessed when the file certificate is verified using the random key and the encrypted electronic file is decrypted using the random key; and

binding firmware to the computing device by an asymmetric manufacture certificate in the externally-accessible memory.

Claim 8. (currently amended) The method of claim 7 wherein the associating step includes the step of generating a software signature encrypted using the random key and storing the software signature in the digital certificate; wherein the software signature is a signature for the electronic file that is symmetrically encrypted using the random key.

Claim 9. (original) The method of claim 8 wherein the generating step comprises the step of generating a hash of the electronic file, where the hash is symmetrically encrypted using the random key.

Claim 10. (original) The method of claim 8 wherein the associating step includes the step of generating a signature for selected fields of the digital certificate,

wherein the selected fields of the digital certificate are coded and encrypted using the random key.

Claim 11. (cancel)

Claim 12. (currently amended) The method of claim 7 and further comprising the step of storing the ~~encoded~~ encrypted key in the externally-accessible memory.

Claim 13. (currently amended) The method of claim 7 and further comprising the step of symmetrically decrypting the ~~encoded~~ encrypted key using the secret identification number upon a request to access the electronic file.

Claim 14. (currently amended) The method of claim 13 and further comprising the step of decrypting one or more fields of the digital certificate using the ~~encoded~~ encrypted key.

Claim 15. (currently amended) The method of claim 14 and further comprising the step of decrypting an encrypted electronic file using the ~~encoded~~ encrypted key.

Claim 16. (currently amended) A method of storing a protected file in an externally-accessible memory of a computing device comprising the steps of:

storing a secret identification number for computing device in a secure memory that is not externally-accessible;

generating a random key associated with a selected electronic file to be stored in the externally-accessible memory;

generating an encrypted ~~encoded~~ key by symmetrically encrypting the random key using the secret identification number;

optionally encrypting the selected electronic file using the random key and storing the encrypted electronic file in the externally-accessible memory; and

storing the encrypted key in the externally-accessible memory and associating the encrypted key with the encrypted electronic file, such that the encrypted electronic file can be decrypted only after restoring the random key through decryption of the encrypted key with the secret identification number; and

binding firmware to the computing device by an asymmetric manufacture certificate in the externally-accessible memory.

Claim 17. (original) The method of claim 16 and further comprising the step of storing an encrypted software signature for the electronic file in the externally-accessible memory, where the software signature is a hash of the electronic file, encrypted using the random key.

Claim 18. (new) A device with a security system for electronic files including a platform certificate comprising:

a processing system;

an externally-accessible memory coupled to the processing system;

a secret identification number generated for the computing device and stored in a secure memory that is not externally-accessible;

a key generator for generating a random key associated with a selected electronic file to be stored in the externally-accessible memory;

a symmetrical encryption system to generate an encrypted key by

symmetrically encrypting the random key using the secret identification number;

wherein the processing system associates a digital certificate with the electronic file, where the digital certificate contains the encrypted key, such that the electronic file can be accessed only after the processing system restores the random key through decryption of the encrypted key with the secret identification number;

wherein the random key is used to sign the file certificate, the electronic file is optionally encrypted using the random key, the electronic file is accessed when the file certificate is verified using the random key and the encrypted electronic file is decrypted using the random key; and

wherein the platform certificate decouples encryption from modification prevention and authentication of the electronic file.

Claim 19. (new) The computing device of claim 18 wherein the random key directly encrypts the electronic file, without an additional level of encryption.

Claim 20. (new) A device with a security system for electronic files including a manufacturer certificate comprising:

a processor;

an internal permanent memory in the processor;

the internal permanent memory for storing a first manufacturer's public key, wherein the first manufacturer's public key is optionally hashed and cannot be modified after writing into permanent memory;

an externally-accessible memory coupled to the processor;

the externally-accessible memory comprises the manufacturer certificate for asymmetric encryption and for prevention of firmware modification and copying; wherein the manufacturer certificate comprises a second manufacturer's public key; and

the processor for comparing the first and second manufacturer public keys and generating a pass or fail output to indicate a match.

Claim 21. (new) The device of claim 20 wherein a hashed value of the second manufacturer's public key is stored in the manufacturer certificate.